

الأمن السيبراني

Cyber Security





بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

(وَلَقَدْ خَلَقْنَا الْإِنْسَانَ وَنَعْلَمُ مَا تُوَسْوِسُ بِهِ نَفْسُهُ
وَنَحْنُ أَقْرَبُ إِلَيْهِ مِنْ حَبْلِ الْوَرِيدِ * إِذْ يَتَلَقَّى الْمُتَلَقِّيَانِ
عَنِ الْيَمِينِ وَعَنِ الشِّمَالِ قَعِيدٌ * مَا يَلْفِظُ مِنْ قَوْلٍ
إِلَّا لَدَيْهِ رَقِيبٌ عَتِيدٌ).

سورة ق



حقيبة الأمن السيبراني التوعوية



حقوق الملكية الفكرية حقوق هذه المادة بالكامل محفوظة لصالح "المؤلف بالملحق ب" وبالتالي يملك في سبيل ذلك حقوق مادية وأدبية ويحظر التصرف فيها بأي شكل أو التعديل عليها بالحذف أو التغيير أو الإضافة أو طباعتها أو ترجمتها أو تسجيلها أو عرضها أو تقديمها أو نشرها أو تصويرها أو أي شكل من أشكال التصرفات المخالفة لنظام حماية حقوق المؤلف وحماية الملكية الفكرية المتعارف عليها دولياً.

الصفحة	الموضوع	م
٧	كلمة افتتاحية	١
٨	مقدمة حقيبة الأمن السيبراني التوعوية	٢
١٠	إرشادات وقواعد العمل والمشاركة بالبرنامج التدريبي	٣
١١	دليل البرنامج التدريبي	٤
١٣	أساليب وأدوات تقييم البرنامج	٥
١٤	مستلزمات البرنامج	٦
١٥	دليل الرموز المستخدمة	٧
١٦	منهاج البرنامج التدريبي	٨
١٧	جدول التعلم الذاتي	٩
١٨	التقويم الذاتي القبلي	١٠
١٩	حقائق وأرقام إحصائية إلكترونية	١١
٢٢	الجلسة الأولى: الفضاء السيبراني	١٢
٢٧	النشاط الأول	١٣
٢٨	الجلسة الثانية: أخطار التواجد بالفضاء السيبراني وأثره على سلوكيات المستخدم	١٤
٣٢	الجلسة الثالثة: الحماية بالفضاء السيبراني	١٥
٣٧	النشاط الثاني	١٦
٣٨	الجلسة الرابعة: حماية المعلومات والخصوصية بالفضاء السيبراني	١٧
٤٥	النشاط الثالث	١٨
٤٦	الجلسة الخامسة: إرشادات تطبيق التواجد الأمن بالفضاء السيبراني	١٩
٥٢	النشاط الرابع	٢٠
٥٥	خاتمة	٢١
٥٦	استبانة تقييم البرنامج التدريبي	٢٢
٥٧	التقويم الذاتي البعدي	٢٣
٥٨	المراجع	٢٤
٦٠	الملاحق	٢٥

الفضاء السيبراني هو الفضاء الذي يعد عالماً افتراضياً نعيشه بواقعنا الحاضر وجزء من حياتنا اليومية حيث يتيح لنا فرصة العمل والتعلم والتواصل والمشاركة لكثير من المعلومات مع الأصدقاء والغرباء في كثير من الأحيان. ومع الإنتشار السريع في التقنيات الحديثة



وتوفر برامج التواصل الاجتماعي على المنصات المتعددة بين مختلف أنواع المستخدمين جعلت هذا الفضاء ساحة إلكترونية متاحة للصغير والكبير والمتعلم وغير المتعلم والسوي صاحب النوايا الحسنة وكذلك غير السوي ذو الطباع السيئة وظهرت لدينا عدة سلوكيات غير

سليمة يصنف بعضها كجرائم معلوماتية، ومن هنا توجب علينا أن نتعلم كيف يكون التواجد الآمن في هذه البيئة الغير منتهية الأطراف والتي تجعل من العالم قرية صغيرة بين أيدينا نجوبها عبر أجهزة هواتفنا الذكية ونشارك بها بياناتنا ومعلوماتنا بشكل يؤثر على خصوصياتنا وسرية تعاملاتنا وبشكل قد يضعنا في فخ الخداع والتلاعب والسرقات الإلكترونية والاختراقات المؤذية والوقوع في المخالفات المعلوماتية والإلكترونية.

د. علي بن عيدروس بن علي البار
وكيل الكليات والمعاهد للتعليم الإلكتروني
الهيئة الملكية ببنبع

اعتاد الناس التواصل في نطاق فيزيائي مكاني مرني ومحدود، لنرى بعضنا البعض وجهاً لوجه وتجاوز ونردش وتفاعل ضمن مساحات معروفة، ولكن مع تطور التقنيات والاتصالات نشأ لدينا ما يعرف بالفضاء السيبراني والذي قد غير من طريقة حياتنا وتعاملاتنا بشكل كبير وأصبحنا نتواصل مع بعضنا البعض في فضاء افتراضي واسع بلا حدود، نرى فيه الصديق والغريب والكبير والصغير والعقل والجاهل وذوي النوايا الحسنة



وغير الحسنة. فقد أثرت هذه البيئة على سلوك كثير من الناس وجعلت منهم أناس أقل تحفظاً ومنفلتين نحو استخدامات ومشاركات غير محدودة كسرت بها قيود الخصوصية والسرية في حياتنا. كما قد جعلت الكثير من رواد هذه البيئة يلبسون أقنعة متعددة ليخفون بها أنفسهم تحت مظلة الزيف

والمجاملات، وقد خلقت وأخرجت لنا الكثير من المشاهير من لا يملكون الفكر ولا الهدف ولا الرسالة. ومنحت لجميع مستخدميها فرصة الظهور وللأسف جعلت من بعضهم منبراً للتنشويه والتحريض والإساءة ونشر الجهالة، وسهلت لهم فرصة الشهرة من خلال تفسير حلم، أو كشف معلومة، أو تقديم فتوى، أو نشر إشاعة، أو إساءة، أو أي موضوع ملفت للعامة.

اليوم، يجب أن نعلم أن ساحات الاختلاط الأكبر ليست في الأسواق، أو الشوارع، أو النوادي كما يظن الكثير من الناس، بل أصبحت بداخل البيوت، من



خلال استخدام الإنترنت وبرامج التواصل الاجتماعي والألعاب الإلكترونية وساحات الدردشة الإلكترونية وغيرها من التطبيقات. وقد يتسع الأمر ويكون الأثر أكبر عندما نتواجد في هذه البيئة من كل مكان وفي أي وقت وزمان وهو ما يحدث لنا في عصرنا الرقمي الحديث، فنحن نحمل بأيدينا أجهزة ذكية توفر لنا

خدمات الإنترنت اللاسلكية والتواصل المباشر والحي مع الناس عبر الهواتف النقالة والأجهزة المحمولة، ومن هنا يجب الاعتراف بأن تواجدنا في هذه البيئة السيبرانية ليس خياراً وإنما وسيلة ومطلب من متطلبات الحياة الحديثة.

من خلال هذه الحقبة، سنتعرف على الكثير من المصطلحات الإلكترونية المتداولة في الفضاء السيبراني وكذلك المخاطر المحتملة من التواجد في هذه البيئة الافتراضية وكيف لهذه البيئة أثر على سلوكياتنا وأفعالنا وأقوالنا وحتى أخلاقنا عند التعامل مع الناس خلف أسوار الاتصالات الحديثة



والتطبيقات المتعددة فنحن نعي أن ساحة الفضاء السيبراني لها الكثير من الفوائد، ولكن هناك الكثير من السلبيات والتي قد توصلنا إلى الجرائم المعلوماتية والإلكترونية. كما سنتعلم على وسائل الاستخدام والتعامل الآمن في هذه البيئة السيبرانية وطرق حماية الخصوصية وحماية المعلومات وحماية الفرد والعمل والمجتمع من

العنف والاعتداء والاحتيال الإلكتروني بكافة أنواعهم وأشكالهم وطرقهم والتعرف على كيفية التصدي والإبلاغ عنهم ومنع حدوثهم.

المتدربين/ المتدربات الكرام:

أشكر لكم اختياركم حضور هذا البرنامج التدريبي والذي من خلاله نسعى إلى إكسابكم المهارات والمعارف المتعلقة بأمن المعلومات وأمن التواجد بالفضاء السيبراني سعياً إلى زيادة الوعي لديكم وجعلكم خط الدفاع الأول لمنع المخاطر والهجمات الإلكترونية المحتملة والبقاء في أمان بإذن الله، وحرصاً على تحقيق الهدف المرجو من التدريب فإننا نذكركم بما يلي:

1. التدريب الفعّال هو الذي تشترك فيه جميع المتدربين بطرح الآراء والأفكار والمناقشة الهادفة.
2. العمل ضمن أفراد المجموعة في التمارين الجماعية يوسع دائرة الفائدة.
3. من حق أي متدرب أن يساهم بطرح فكرته أو رأيه.
4. الأفكار عزيزة عند أصحابها حرياً بنا أن نتصت لها.
5. أنماط التفكير تختلف من شخص لآخر.
6. الحضور في الوقت المحدد للبرنامج من عوامل النجاح.
7. التركيز على التدريب وتجنب المعوقات - كالجوال ونحوه - يوسع دائرة الاستفادة.
8. تقبل الدور الذي يسند إليك في المجموعة من عوامل نجاح إنجاز المهمة.
9. الخبرة في ذاتها وبذاتها ليس لها معنى إلا إذا استعملت.
10. ليس هناك فشل ولكن تجارب وخبرات وفرص للتعلم.
11. كم هو جميل أن نحرص على بناء علاقة طيبة مع المدرب والزملاء أثناء البرنامج التدريبي.
12. إن تحفيز أفراد مجموعتك في المشاركة في النشاطات يقوي فرص النجاح لديكم.
13. إن انتقل أثر التدريب وتطبيقه في البيئة العملية دليل نجاح.

اسم البرنامج:

حقيبة الأمن السيبراني التوعوية



الهدف العام للبرنامج:

توعية المتدربين بكيفية التواجد الأمن ضمن بيئة الفضاء السيبراني

وصف البرنامج التدريبي

برنامج تدريبي يهدف إلى مساعدة المستخدمين/ الموظفين على كيفية التعامل مع الانترنت من خلال ممارسة الأنشطة في البرنامج وتعزيز حماية وسرية وخصوصية البيانات الشخصية والعملية واتخاذ جميع التدابير اللازمة لتجنب المخاطر المحتملة في الفضاء السيبراني.

ماهي أهداف حقيبة الأمن السيبراني التوعوية؟

تتبلور أهمية الحقيبة التدريبية فيما يلي:

- التعريف بمصطلحات الفضاء السيبراني العامة والمعاني الخاصة
- توضيح أخطار الفضاء السيبراني ومنصات التواصل الاجتماعي
- بيان سبل تحقيق الأمن السيبراني الشامل
- ممارسة مبادئ وأساسيات الأمن السيبراني
- التعرف على الاستخدام الأمن والمشاركة الأمانة للمعلومات
- استشعار المخاطر التي تعصف بمنصات التواصل الاجتماعي
- توضيح أهمية القيم في تحقيق الفائدة من استخدام الفضاء السيبراني
- توضيح طرق مكافحة الجرائم المعلوماتية بالمملكة العربية السعودية



الفئة المستهدفة:



منسوبي الهيئة الملكية للجبيل وينبع

مدة البرنامج:



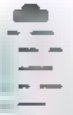
يوم واحد (5 ساعات تدريبية)

الوسائل المقترحة:



عروض تقديمية – ورش عمل – نشاطات – جلسات نقاش وحوار.





التقويم الذاتي القبلي.

يمكن الوصول عبر مسح الكود الظاهر.



تقويم البرنامج التدريبي

(استمارة تقويم البرنامج من حيث الأهداف، المحتوى، الأساليب، المدرب، بيئة التدريب، الوقت) يمكن الوصول عبر مسح الكود الظاهر.



التقويم الذاتي البعدي.

يمكن الوصول عبر مسح الكود الظاهر.





مقدمة ٢٠ دقيقة	الافتتاح ومقدمة البرنامج	
إحصاءات ٢٥ دقيقة	حقائق وأرقام إحصائية إلكترونية	
الجلسة ١ ٣٠ دقيقة	الفضاء السيبراني	الجلسة الأولى
نشاط ١ ٢٠ دقيقة	الحقائق والاعتقادات الخاطئة	النشاط الأول
استراحة: ٢٠ دقيقة	استراحة	
جلسة ٢: ٢٥ دقيقة	أخطار التواجد بالفضاء السيبراني وأثره على سلوكيات المستخدم	الجلسة الثانية
جلسة ٣: ٢٠ دقيقة	الحماية بالفضاء السيبراني	الجلسة الثالثة
نشاط ٢: ٢٥ دقيقة	جدة الاعتراف	النشاط الثاني
استراحة: ٢٥ دقيقة	استراحة	
جلسة ٤: ٢٠ دقيقة	حماية المعلومات والخصوصية بالفضاء السيبراني	الجلسة الرابعة
نشاط ٣: ٢٠ دقيقة	الهندسة الاجتماعية	النشاط الثالث
جلسة ٥: ٢٠ دقيقة	إرشادات تطبيق التواجد الآمن بالفضاء السيبراني	الجلسة الخامسة
نشاط ٤: ١٥ دقيقة	مقياس الممارسات الإلكترونية الخاطئة	النشاط الرابع
خاتمة: ١٠ دقيقة	الوصايا العشر في الأمن السيبراني	خاتمة
استبانة: ٥ دقائق	استبانة تقييم البرنامج التدريبي	استبانة

جدول التعليم الذاتي KWL-Q

الجدول الذاتي في الملحق (أ) يساعد على أن تتأملوا فيما تعرفون حول موضوع التدريب، وما تريدون معرفته، وما ستتعلمون خلال هذا التدريب بعد كل جلسة ونشاط تدريبي.

- 1- في بداية التدريب سجل في العمود الأول ما تعرف عن موضوع التدريب (Know)، وفي العمود الثاني سجل ما تريد أن تعرف (Want to Know).
- 2- خلال التدريب اكتب في العمود الثالث ما تعلمته (Learned).
- 3- في حالة وجود أسئلة لديك خطرت في بالك ولم تجد الإجابة عليها أثناء التدريب، فاكتب أسفل الجدول (Question) حتى تبحث عن إجاباتها أو تقوم بطرحها على المدرب خلال البرنامج التدريبي.

L	W	K
ماذا تعلمت؟	ماذا أريد أن أعرف؟	ماذا أعرف؟

أسئلة لازالت لدي (Q) ؟

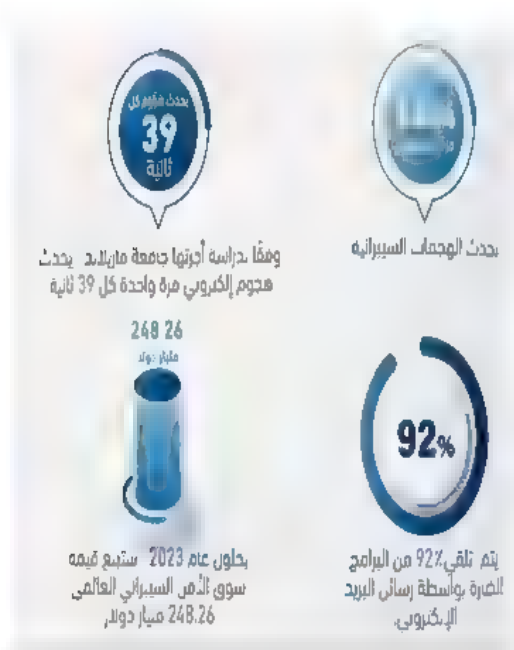
استبانة التقويم القبلي لقياس وعي المستخدمين بمفاهيم الأمن السيبراني.

أرجوا قراءة العبارات التالية والإجابة بـ (نعم) حال الموافقة على ما تم ذكره بالعبارات والإجابة بـ (لا) حال عدم الموافقة عليها:

لا	نعم	العبارة
		أقوم باستخدام برمجيات وتطبيقات خاصة لحماية جهازي من الاختراق والتجسس والفيروسات
		أحتفظ بالبيانات الخاصة بي في أكثر من مكان لتفادي فقدانها أو تلفها
		أقوم بنسخ البيانات الخاصة بي احتياطياً في ذاكرة خارجية وحفظها بمكان آمن
		أسمح بمشاركة معلوماتي الشخصية للأصدقاء عبر الإنترنت وبرامج التواصل الاجتماعي وغيرها من الوسائل بالفضاء السيبراني
		أسمح بمشاركة معلوماتي الشخصية للغرباء عبر الإنترنت وبرامج التواصل الاجتماعي وغيرها من الوسائل بالفضاء السيبراني
		أسمح بمشاركة بعض معلوماتي الشخصية غير الحساسة للأصدقاء عبر الإنترنت وبرامج التواصل الاجتماعي وغيرها من الوسائل بالفضاء السيبراني
		أسمح بمشاركة بعض معلوماتي الشخصية غير الحساسة للغرباء عبر الإنترنت وبرامج التواصل الاجتماعي وغيرها من الوسائل بالفضاء السيبراني
		أحرص على تجنب مشاركة المعلومات المخالفة للعقيدة، أو الدين، أو القوانين، أو الاعراف، أو التقاليد
		دائماً ما أراعي آراء الآخرين ومشاعرهم عند مناقشة موضوع ما عبر الإنترنت
		لدي وعي كافي بأنظمة المملكة العربية السعودية المتعلقة بالأمن السيبراني يمكنني من التعامل مع الإنترنت وبرامج التواصل الاجتماعي بشكل آمن وصحيح
		أشدد على ضرورة توعية المستخدمين/ الموظفين/ الطلبة بمفاهيم الأمن السيبراني والتطبيقات والقوانين والمخالفات والعقوبات المتعلقة باستخدام الإنترنت وبرامج التواصل الاجتماعي
		أؤيد وضع إجراءات وسياسات واضحة لحفظ الأمن السيبراني الخاصة بمشاركة المعلومات ونقلها عبر الإنترنت

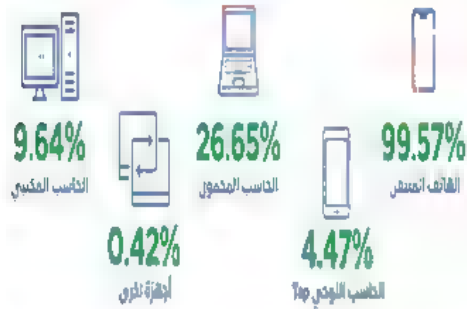


حقائق وأرقام إحصائية إلكترونية

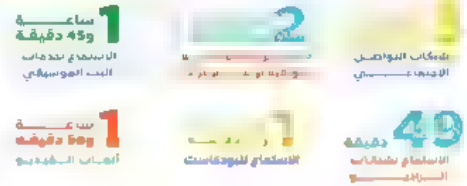


الأجهزة المستخدمة للوصول إلى الإنترنت

نسبة إلى عدد مستخدمي



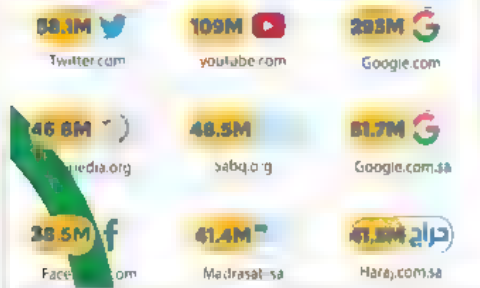
وقت متابعة الإنترنت والوسائط المتعددة يوميًا



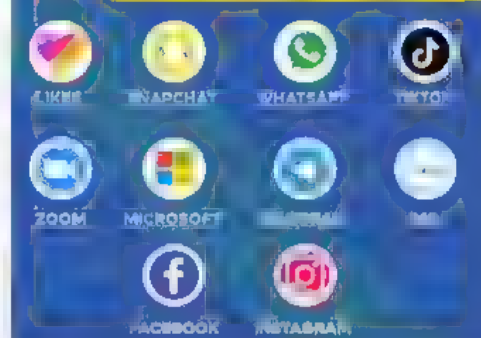
طرق البحث على الإنترنت

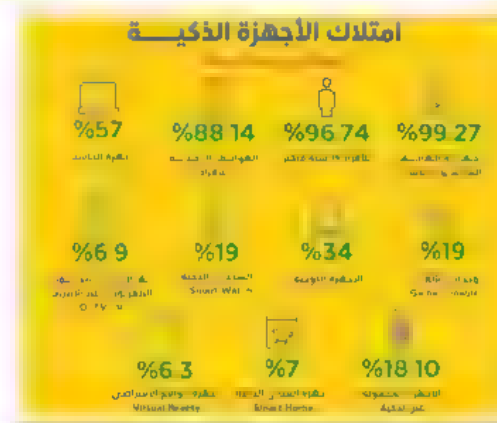
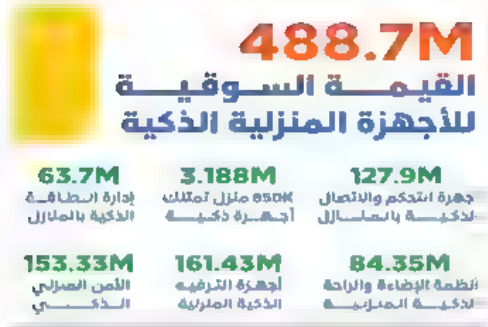


أكثر المواقع تصفحًا



أعلى التطبيقات تحميلًا





المصدر: TREND | Digital Communication
يمكن الوصول للتقرير من خلال الرابط: https://trenddc.com/report/saudi_digitization2021

الجلسة الأولى



ماذا نقصد بالفضاء السيبراني Cyber-sphere؟

كلمة فضاء (Sphere) تعني الساحة والتي يمكن أن تكون مساحة للتواجد فيما بيننا وعند إضافة كلمة سيبر (Cyber) فتصبح ساحة الإنترنت أو الوصلة الرقمية التي تضيف خاصية تكنولوجيا المعلومات وبها تكسر قيود الزمان وحدود المكان فتعطي إمكانية التواصل الإلكتروني على شبكات الإنترنت، وتجمع الأصدقاء مع الأصدقاء وقد يكون مع الغرباء، والتواصل في هذه الساحة الافتراضية على هيئة تبادل وتشارك أنواع مختلفة من الرسائل بين المستخدمين ومنها على سبيل المثال تبادل الرسائل النصية والصوتية والرسومية الثابتة والمتحركة والفيديوهات وغيرها من الوسائط المتعددة.



إذا هل الفضاء السيبراني حقيقة؟

الجواب المؤكد هو أنه حقيقة ضمن ساحة افتراضية غير ملموسة وهي ليست ساحة محدودة التفاعل مثل بعض الأشياء الأخرى التي اعتدنا على استخدامها مثل مشاهدة التلفزيون، أو إجراء مكالمات هاتفية، أو الاستماع إلى الراديو، بل أصبحت بيئة ينغمس فيها الشخص ذهنياً إلى درجة كبيرة فتستحوذ عليه بطريقة فريدة وتجذبه إليها حيث ينسى واقعه الذي يعيشه. كما أن هذا الفضاء مليء بأسماء الأماكن وشبكات التواصل الاجتماعي والمنديات والمواقع الإلكترونية والألعاب الإلكترونية وغير ذلك وحين نتواجد هناك ننضم إلى مجموعات كبيرة من الأشخاص من قد تربطنا بهم علاقة أو قد لا نعرفهم أصلاً، وهذا ما يجعل من هذه البيئة فريدة من نوعها لتكسر كثير من الحواجز.



هل هناك آثار إيجابية أو سلبية من تواجدنا في الفضاء السيبراني؟

قد نعلم أن هنالك فوائد كثيرة من التواجد في الفضاء السيبراني فقد وجدنا أنفسنا أمام خيارات متعددة ومفيدة خلال جائحة فيروس كورونا المستجد كوفيد-19 فعلى سبيل المثال كان هنالك خيارات العمل عن بعد وعقد الاجتماعات الافتراضية



وكذلك التوجه إلى التعليم عن بعد من خلال المنصات المختلفة وإتاحة حضور الفصول الافتراضية واستكمال عملية التعليم والتعلم دون توقف وقد زادت هذه الحلول من زيادة الأمان الصحي والرعاية المجتمعية والائتمان الاقتصادي وغيرها من الفوائد ولكن في الوقت ذاته ظهرت لدينا الكثير من المخاوف والإشكالات وذلك بسبب إما قلة الوعي باستخدام الأدوات التقنية والتعامل معها

ومعرفة الاستخدام الصحيح لها وطرق حفظ الخصوصية ومشاركة المعلومات أو لأسباب عدم فهمنا الواسع للبيئة السيبرانية وإدراك مخاطرها المحتملة وما يترتب على ذلك من عقوبات وغرامات وغيرها من الأمور الخطيرة.



من هنا يجب أن نعي أن هناك آثار سلبية من التواجد في هذه الساحة الافتراضية وهنالك فرص للتعرف والالتحاق بشبكات واسعة من الأشخاص وكم كبير من الاتصالات التي تفتح حياتنا وخصوصياتنا في كل وقت وحين، وكيف من الممكن أن يتغير سلوكنا عندما ندخل في هذه الساحة الافتراضي، فقد تخذلنا الغرائز ويتغير سلوكنا عما كنا عليه في الواقع الحقيقي مع الناس وجهاً

لوجه، وقد نجد أنفسنا لنتعامل مع أشخاص مختلفين عنا اجتماعياً وثقافياً ودينيّاً وسلوكياً، فهي ساحة تخدم روادها إن أحسنوا استعمالها ولها جانب مظلم يجب أن نحذر منه خصوصاً عندما نواجه بعض ضعفاء النفوس وغير الأسوياء والشواذ والمجرمين والغامضين والحاquدين والشرسين وللأسف فهم يجدونها ساحة جاذبة لهم ليختفوا خلفها بحجة اللهو واللعب والدرdشة ويستغلوا ضحاياهم ويتعاملوا معهم وكأن الأشياء الغير مقبولة في الواقع الحقيقي مقبولة والأفعال الغير مسموحة مسموحة وهو الأمر الذي يشكل الخطر الكبير في هذه الساحة الإلكترونية لنرى الكثير من السلوكيات الغير سوية مثل التتمر الإلكتروني والتسلط والإيذاء والترهيب والابتزاز والكراهية والعدوانية وفي نهاية المطاف إلى ما يفضي إلى الجريمة الإلكترونية والمعلوماتية.

فماذا نقصد بالتنمر والتسلط والإيذاء الإلكتروني Cyberbullying ؟

لا نعني بالتنمر أن يكون الشخص نمرأ، وإنما أن يصبح سلوكه عدانياً شرساً فظاً ذو أخلاق سيئة، فيختار المعتدي من هو أضعف منه جسدياً أو نفسياً أو أعلى مكانةً وسلطة وقوة لكي يؤذيه



بطرق متعددة. فهو سلوك عداني متعمد ويحدث بشكل مكرر من جانب شخص واحد أو مجموعة من الأشخاص غرضهم إيذاء الآخرين من خلال استخدام الوسائل الإلكترونية في الفضاء السيبراني وهم في حالة وعي تام. وتتمثل هذه السلوكيات في إصاق التسميات غير اللائقة، إرسال الرسائل المهينة وغير مرغوب

فيها، نشر الإشاعات والمعلومات المغلوطة عن الضحايا، ونشر الصور ومقاطع الفيديو المحرجة، والتي غالباً ما تسبب الشعور بعدم الارتياح والحرع الشديد والألم النفسي والمعنوي للضحية.

وماذا نقصد بالترهيب والتخويف والتتبع الإلكتروني Cyberstalking ؟



الترهيب الإلكتروني عبارة عن مجموعة من الأفعال والسلوكيات على الإنترنت وتحدث في ساحات الفضاء السيبراني موجهة إلى شخص معين تصيبه بالقلق والشعور بالخوف وعدم الراحة. ومن الأمثلة إرسال رسائل عدوانية غرضها الابتزاز أو التخويف والترهيب ونشر معلومات كاذبة وشائعات سيئة واقتراءات قد تدمر الوضع الاجتماعي

للضحية، وكذلك تتبع الضحية لجمع معلومات قد تؤثر على علاقاته الشخصية والعائلية والمهنية الحالية والمستقبلية وقد ترتبط بأنواع مختلفة من الابتزاز وطلبات أفعال أمور محددة والامتناع عنها وقد يرتبط ذلك بمطالبات مالية ومادية.

وماذا نقصد بالممارسات الإلكترونية الخاطئة؟

الممارسات الإلكترونية الخاطئة تتمثل في الاستخدام غير الامن لبرامج التواصل الاجتماعي (فيسبوك، تويتر، سناب شات، إنستغرام، تيك توك، وغيرها) وتبادل المعلومات الشخصية والمعلومات الحساسة والسرية عبر هذه التطبيقات بشكل غير آمن. كما أن حساسية المعلومات تعتمد على مدى أهمية وسرية المعلومات المتبادلة فقد يكون نشر الصور الشخصية ومقاطع الفيديو الخاصة وما تحتويه من قضايا أسرية واجتماعية وصحية وخطط مستقبلية وأسرار شخصية، أو عائلية، أو مهنية، أو مالية نوع من الممارسات الخاطئة. إضافة إلى ذلك تجاهل الإعدادات الصحيحة لحماية الخصوصية ضمن هذه التطبيقات وإتاحة المعلومات للعوام، وأيضاً استخدام هذه البرامج في نشر المعلومات الغير صحيحة والشائعات من دون التأكد من مصدرها وتجاهل السياسات والقوانين والأنظمة والعقوبات المترتبة.



إحصائيات عامة عن العدوانية الإلكترونية



المصدر: مبادرة العطاء الرقمي

يمكن الوصول للمصدر من خلال الرابط: <https://cyberbullying.attaa.sa>

يتم توضيح الحقائق وتصحيح الاعتقادات الخاطئة الأكثر شيوعاً في الفضاء السيبراني من خلال شرح ١٦ عبارة يعتقد بصحتها.



يقوم المتدرب بقراءة العبارات، ويقوم بوضع العلامة (✓) إذا كانت العبارة صحيحة وتحاكي الواقع أو العلامة (X) إذا كانت تمثل مفهوم سائد واعتقاد خاطئ.



بعد ذلك يقوم المدرب بشرح كل عبارة وتوضيح لماذا هي حقيقة أو مفهوم خاطئ وتبيان أثار هذا الاعتقاد على سلوكيات الناس ومدى المخاطر المحتملة من ذلك في الفضاء السيبراني.



يمكن الوصول للنشاط من خلال الرابط:

<https://fs7.formsite.com/alibaro/j5guen8w7l/index.html>



خطأ	صحيح	العبارات
		بشكل عام، العدوانية جزء طبيعي من نمو الفرد متطلب لبناء الشخصية وينتهي دون تدخل معظم حالات العدوانية السيبرانية تكون لفظية ومن مصدر خارجي لا يستدعي الفلق في كثير من الأحيان يولد الإنسان بطبيعته متمراً أو عدائياً متحيزاً
		المتنمرون يتخلصون من سلوكياتهم العدوانية باستخدام التقنية ودون قصد الإيذاء المتنمرون هم ذوي مهارات اجتماعية ممتازة ولديهم صداقات وثقة عالية بأنفسهم عادة ما يكون هناك آخرون يشهدون وقوع حالات التنمر والعدوانية المتنمرون يعانون من تدني احترام الذات ويتم رفضهم من قبل أقرانهم أو المجتمع يجب أن يكون هنالك شخصية الضحية لتتم حالة التنمر والعدوانية ضحايا التنمر يجب عليهم الوقوف بشدة ومهاجمة المتنمرين بالمثل وضع القوانين يساهم في الكشف والحد من حالات العدوانية السيبرانية الاعدادات التقنية ستحمي المستخدمين من حالات العدوانية السيبرانية مسؤولي تقنية المعلومات عليهم مسؤولية حماية المستخدمين ومنع العدوانية السيبرانية لم تعرض للعدوانية السيبرانية فاعتقد بعدم وجودها ولا تستحق الاهتمام العدوانية السيبرانية لن تتحول الى عدوانية جسدية طالما هي عبر الانترنت العدوانية السيبرانية لن تشكل أخطار على اختراق الأجهزة او المعلومات او الخصوصية العدوانية السيبرانية لا تصل إلى حد تصنيفها من ضمن الجرائم المعلوماتية

الجلسة الثانية



أخطار التواجد بالقضاء السيبراني وأثره على ملوكيات المستخدم

ما هي الجرائم الإلكترونية والمعلوماتية Cybercrimes ؟

هي المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء الضحايا أو تحقيق أذى مادي أو نفسي لهم، إما بشكل مباشر أو غير مباشر وذلك باستخدام شبكات الاتصالات والإنترنت وعبر منصات وبرامج التواصل الاجتماعي وغرف الدردشة ضمن الألعاب والبريد الإلكتروني وعبر تطبيقات الهواتف الذكية والأجهزة اللوحية وما شابهها، وفيما يلي بعض الأمثلة لتلك الجرائم:



- 1 الاستهزاء والتشهير
بالآخرين وتشويه
السمعة وإلحاق الضرر
بالضحايا
- 2 الاختراق وسرقة
المعلومات وتزييفها
والإتجار بها
- 3 سرقة الحسابات
وانتهك الخصوصية
وانتحال الشخصية
- 4 التهريب والتهديد
والابتزاز؛ وحمل
الضحايا على القيام
بفعل عمل ما أو
الامتناع عنه
- 5 التمر والتسلط والأذية
ونشر الكراهية والعنف
بين أفراد المجتمع
- 6 التحرش والمضايقة
لكافة فئات المجتمع من
الجنسين وشتى
الأعمار
- 7 جمع ونشر الصور
والمقاطع الإباحية
الهادمة للقيم الدينية
والآداب العامة في
المجتمع
- 8 هدم القيم الأسرية
والمواطنة ونشر
العنصرية بين أفراد
المجتمع

وليس من المستغرب وجود هذا الكم الكبير من المخالفات في هذا الفضاء الافتراضي الواسع وما قد يحدث به في الحقيقة هو ليس من الأمور الاعتيادية كما يعتقد البعض بل هي ممارسات مصنفة بأن تكون من الجرائم استناداً على نظام مكافحة جرائم المعلوماتية بالمملكة العربية السعودية والذي تم إقراره في مجلس الوزراء السعودي رقم 79 وتاريخ 1428/3/7 هـ، وتمت المصادقة عليه بموجب المرسوم الملكي الكريم رقم 17 /م وتاريخ 1428/3/8 هـ، والذي يهدف إلى الحد من وقوع الجرائم الإلكترونية والمعلوماتية وقد سنت به العقوبات الصارمة والتي قد تصل إلى السجن لمدة ١٠ سنوات في أقصاها وغرامات مالية قد تصل إلى ٥ ملايين ريال في حدها الأعلى. للاطلاع وتفاصيل أكثر عن النظام يرجى نسخ الكود الظاهر.



ماذا بعد ذلك؟ هل التواجد في الفضاء السيبراني يعتبر امناً؟



لعله من أحد أهم الأسئلة التي تدور بالأذهان، ولكن يجب أن نعي أن الفضاء السيبراني ساحة جامعة لمختلف النوعيات من البشر ونعلم أن الأطفال والشباب هم أكثر عرضة لمخاطر الفضاء السيبراني ومن الطبيعي أن يشعروا بالفضول وقد يريدون استكشاف كل جديد وفي الواقع هم لا تنقصهم الخبرة في استخدام التطبيقات المختلفة، بل قد يفوقون الكبار براعة في استخدامها، ولكن ليس لديهم النضج الكافي لإدراك المخاطر المحتملة ونتائج التعامل والتواصل المفتوح في هذه البيئة الافتراضية. الساحة السيبرانية تتضمن الاحتكاك ببعض الغرباء والناس الخطيرين، وهؤلاء كثيراً ما لا يخضعون للمراقبة فهم في ساحة يعلمون أن الأطفال أحد ضحاياها ويتعرضون فيها للمخاطر والإهمال في الوقت ذاته.

ويعتبر ذلك من أخطر سلبيات التعامل في هذه البيئة المفتوحة والتي بدورها تغير من سلوكيات الناس ومشاعرهم وقيمهم وإخفاء هويتهم الحقيقية، وكيف يستغل المجرمون تلك التغيرات فلربما نعلم بعض الأشياء عن انتحال الهوية، التلصص، التحرش، السرقات للحسابات وبذلك نضع كلمات سر خاصة وقوية لضمان الأمان قدر الإمكان ولكن لربما لا ندرك كيف أننا نسهم من خلال بعض الممارسات الخاطئة في احتمال تعرضنا المباشر للخطر لكي نقع في فخ التنمر أو الترهيب أو الابتزاز ... فعلى سبيل المثال عندما نجلس في غرفة النوم ونحن نخبر العالم كله في فيسبوك، تويتر، سناب شات، إنستغرام وغيرها من التطبيقات بكل شيء فعلناه في ذلك اليوم ونشاركهم الصور والمقاطع الطريفة لمناسباتنا ومقابلاتنا العائلية وحتى الوجبات الشهية وغيرها من الأحداث الخاصة، بينما عندما نكون في السوبرماركت مثلاً، فلن نخبر أي غريب أو مجهول نراه وجهاً لوجه عن تلك الأشياء.

والسؤال الذي يطرح نفسه لماذا يحدث هذا لنا في هذه الساحة السيبرانية؟

الجواب المثير للاهتمام هو أننا في الحقيقة ننسى أنفسنا في لحظات وربما نطلع ملايين الغرباء على خصوصياتنا بسبب تأثيرات عدم الإحساس بالتحفظ في الفضاء السيبراني. من هنا يجب علينا التفكير بما سنشاركه مع الناس في هذا الفضاء السيبراني، فأنت تملك المعلومة وهي خاصة بك حتى تقوم بالنقر على زر إرسال أو مشاركة، عندها ستكون ملك للغير وليست من ممتلكاتك الشخصية كما كانت. كما أن هنالك دور كبير على الآباء والأمهات وكل رب أسرة وكل راع فهم شركاء أساسيين في حماية أبنائهم وذويهم على الإنترنت. ويجب أن يكون دخول كل ابن وابنة لساحة الفضاء السيبراني ضمن حدود وصلاحيات ورقابة عالية من الوالدين فقد يتعرضون للكثير من المضايقات وهم يمارسون الألعاب الإلكترونية من خلال الدردشة أو عند استخدام برامج التواصل الاجتماعي ومشاركة المعلومات وهي في الحقيقة قد تكون جرائم في حقهم مؤثرة بشكل سلبي على حياتهم الأسرية والاجتماعية والعلمية وغيرها من الجوانب والتي قد تسبب الضرر النفسي والجسدي إن لم يحسن التصرف وأخذ التدابير الصحيحة ومعالجتها ومنعها منذ بداياتها.

ما هو العمر المناسب للتواجد بالفضاء السيبراني واستخدام برامج التواصل الاجتماعي والألعاب الإلكترونية؟

معظم التطبيقات والألعاب تم تصنيفها بناء على المحتوى الذي يمكن مشاهدته من خلالها ولذلك تم تصنيف البرامج الأكثر انتشارا واستخداما حسب التصنيف العمري التالي:



انستقرام

+12



يوتيوب

+17



تويتر

+17



سناپ شات

+12



تيك توك

+12



فيس بوك

+12

الجلسة الثالثة



ماذا نعني بالأمن السيبراني؟

"هو مجموعة من التقنيات التي تقوم بحماية وسلامة الأجهزة والشبكات والبرامج والبيانات من الهجوم والتلف أو الوصول غير المصرح به، ويمتد إلى أنه مجموعة من الأدوات والسياسات والمفاهيم الأمنية، وضمانات الأمان والمبادئ التوجيهية التي تدير على نهج إدارة المخاطر والإجراءات، وتعد أفضل الممارسات والضمانات التقنية التي تستخدم لحماية أصول المنظمة والمستخدم" (المبيض، ٢٠٢٠، ص: ١٣).



تعزيز توافر البيانات
للمستخدمين المصرح لهم

الحفاظ على
سلامة البيانات

حماية
سريته البيانات

كيف أحمي نفسي سيبرانياً؟



الجواب لهذا السؤال يعتبر خارطة الطريق ودليل لبر الأمان عندما نتواجد في ساحة الفضاء السيبراني. ولعل أبسط إجابة لهذا السؤال هو أن نزيد من وعينا ونقوم بزيادة إدراكنا بالأدوات والسياسات والمفاهيم الأمنية المتعلقة بالأمن السيبراني لنعي المخاطر المحتملة ونفهم طبيعة التعامل في هذه البيئة المفتوحة مع مختلف الأنواع من البشر، وعلينا أن نجعل بقاءنا في الفضاء السيبراني ضمن حدود الأمن والأمان.

وفيما يلي سنتطرق إلى عدة محاور ونصائح مهمة تزيد من الوعي المعرفي لدينا. ففي الفضاء السيبراني، ليس كل ما نراه هو حقيقة، فهناك الكثير من المواد التي قد تكون شائعات أو معلومات مغلوطة وبها تزييف للحقائق ويجب أن نعلم ما يلي:



- ليس كل شيء على الإنترنت صحيح ومؤكد

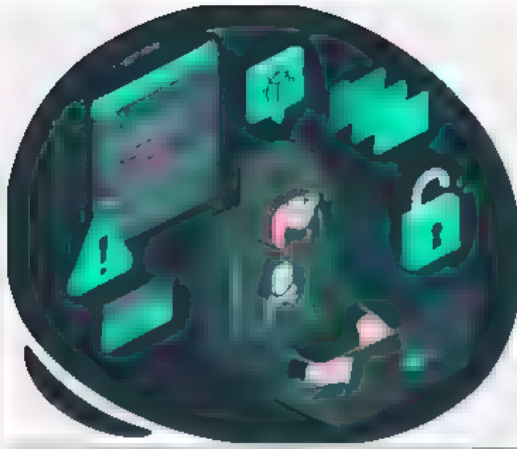
- من نقابلهم على الإنترنت قد يخفون هويتهم ويتعاملون معنا بزييف

- الصور والمقاطع قد تظهر لنا معنى مختلف عن الحقيقة

- كل ما تم وضعه على الإنترنت أصبح ليس ملك لأصاحبه وخاصته

- الخصوصية على الإنترنت أكثر عرضة للكشف فلا مجال للأسرار

مراقبة السلوكيات ضمن البيئة السيبرانية



يجب علينا أن نعلم بأن تأثير البيئة السيبرانية كبير علينا فعندما نتحدث إلى الأشخاص عبر الإنترنت فنحن لا نرى تعابير الوجه ولا لغة الجسد ولا الإشارة وهذا قد يعطينا حرية أكبر لقول أي شيء وفعل أي شيء عكس ما إذا كنا نقابلهم وجهاً لوجه. وكذلك يجب أن نعلم أن من نتعامل معهم في البيئة السيبرانية فهم الأشخاص ذاتهم ولديهم نفس المشاعر والأحاسيس ولا يعني أن تواجههم خلف الشاشات بأسماء مستعارة وبصور

شخصيات كرتونية بأنهم أشخاص مختلفين لا يتأثرون بما نقول أو نفعل أو نشارك.

العواقب المحتملة من تعاملاتنا في الفضاء السيبراني

كل ما نقوم بكتابته أو فعله ضمن الساحة السيبرانية سنتحمل نتيجته. وعليه يجب أن نفكر قبل القيام بأي شيء فما نقوم به سوف يظهر للجميع دون حدود وقد يصل للملايين خلال ساعات. فاحرص على ما يلي:

- * لا تشارك معلوماتك الشخصية والحساسة مثل أرقام الهوية، أرقام الهاتف، عنوان المنزل، معلومات العائلة المالية والخطط المستقبلية وغيرها.
- * لا تشارك ما يزعج الآخرين ويؤذيهم من معلومات، وصور، ومقاطع فيديو، وغيرها.
- * لا تشارك محتويات مخالفة للأداب والقيم والأعراف.
- * لا تشارك ما يثير الفتن والعنصرية والكراهية.
- * لا تستخدم لغة بذيئة وكلمات مبذلة غير مقبولة اجتماعياً.
- * لا تضع مشاركة سينة بهدف حذفك لها لاحقاً فهناك بعض التطبيقات تحفظ هذه المشاركات حتى بعد حذفك لها.
- * عدم السماح والخوض في المحادثات الإباحية مع الأغراب أو الأصدقاء وتبادل الرسائل والصور والفيديوهات الخاصة المخلة للأداب والتي غالباً ما تفضي إلى الابتزاز.
- * أخذ الحذر عند المشاركة في المجموعات والتي تحتوي على عدد كبير من الأشخاص فهي تزيد من احتمالية انتشار المحتوى بشكل سريع ضمن نطاق واسع والتعرض للمساءلة (مثل: تصوير شخص ما لغرض الاستهزاء به ونشر الفيديو ضمن المجموعات).



الآثار المترتبة من الاستخدام السلبي

يمكن أن يؤثر علينا التواجد في الفضاء السيبراني بشكل سلبي إن تم ادمان استخدام برامج التواصل الاجتماعي والألعاب الإلكترونية ومشاركة المعلومات الشخصية والعملية بشكل غير محدود و بلا وعي، ومن الآثار المحتملة ما يلي:

- 01 السيول للعزلة الاجتماعية
- 02
- 03
- 04
- 05
- 06
-
-
- 09
- 10 التعرض لمحاولة الاحتيال





الهدف من النشاط هو تأكيد وصول المعلومة الصحيحة للمتدربين وتعزيز الإدراك للمفاهيم الأساسية.

سيتم إعطاء المتدربين فرصة لكتابة مشكلة قد حدثت لهم عند استخدام برامج التواصل الاجتماعي أو غيرها من الوسائل ضمن ساحة الفضاء السيبراني ومن دون كتابة أسماء أو أي معلومات شخصية عن المشاركين.

رابط الجرة الإلكترونية:

<https://fs7.formsite.com/alibaro/lhvckzckdj/index.html>



يجب على المتدربين وصف المشكلة وأثرها عليهم دون التطرق والحديث عما تم اتخاذه من إجراءات لحل المشكلة ويمكن الاكتفاء بذكر قد انتهت بالحل أو تم إهمالها دون حل.



بعد ذلك يقوم المدرب بجمع المدونات ضمن الجرة الإلكترونية.

يقوم المدرب بفتح بعض المدونات وليس جميعها وقراءتها وبدء النقاش لمعرفة الحلول المناسبة. كما سيتم نقاش المدونات والرد على البريد الإلكتروني حال وجود استفسارات.



الجلسة الرابعة



ماهي أخطار الفضاء السيبراني؟

تتمحور أخطار الفضاء السيبراني في عدد من الأساليب الشهيرة للاختراق وانتهاك الخصوصية، ومنها:



الهندسة الإجتماعية

ملف يملك ويبدو طبيعي
بيما هو عبارة عن برنامج
صت

انتحال على المستخدم
يعرض الحصول على
معلومات المفترض ألا
يفصح عنها

عبارة عن مواقع أو رسائل
بريد إلكتروني من منحل
صممها مطابقة للأصيه
ثم يرونها لعرض الدخيل



الابتزاز الإلكتروني

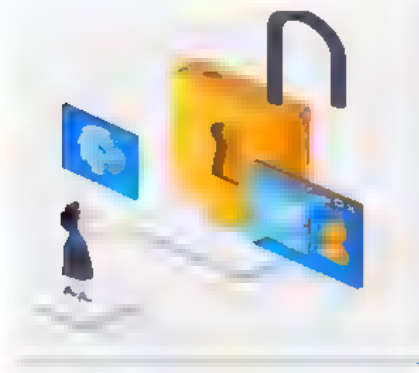
الحصول على معلومات أو
مادة أو صورة إما است طوعا
بالاحتياط أو عن طريق
الهجوم على جهاز الضحية ثم
استخدامها ضده مقابل
الحصول على المال

الاحتيال الإلكتروني

انتحال شخصية أحد
لمشاهير أو لأقارب
الحصول على معلومات
من المفترض ألا تقوم
بالإفصاح عنها

حماية الخصوصية في الفضاء السيبراني

يعرف موقع ويكيبيديا أن الخصوصية في الإنترنت "هي القدرة على تحديد المعلومات التي يكشفها الفرد عن نفسه أو يتحفظ عليها في الإنترنت وتحديد من الذي يمكنه الوصول إليها، ولأي أغراض يمكن أن تستخدم أو الأغراض التي لا يمكن أن تستخدم لها"، ومن هنا يجب علينا حفظ خصوصياتنا لكيلا يتم استغلالها واستخدامها بشكل سيء ومؤذي لنا.



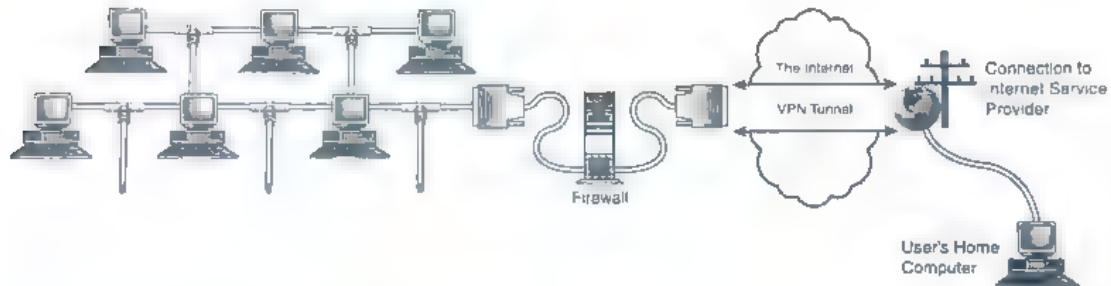
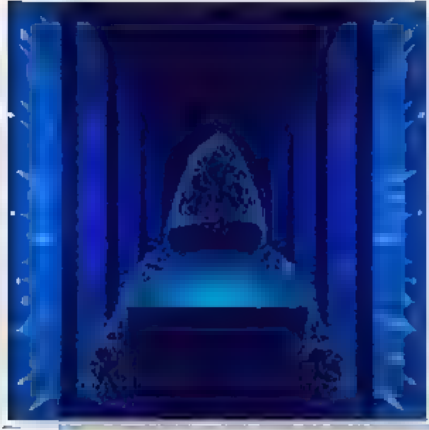
وفيما يلي عدد من النصائح لحفظ الخصوصية بالفضاء السيبراني:

- أن يتم استخدام كلمات المرور عند الدخول على أجهزتنا وجوالاتنا وحساباتنا في برامج التواصل الاجتماعي المختلفة.
- أن يتم استخدام كلمات مرور طويلة وقوية (أكثر من كلمة) وحفظها بشكل آمن وعدم الإفصاح عنها أو مشاركتها مع أي أحد حفاظاً على سريتها.
- تجنب استخدام كلمة مرور واحدة أو متكررة لعدة تطبيقات فإن تمت سرقة كلمة المرور استطاع المخترق سرقة الحسابات الأخرى.
- تجنب استخدام كلمات مرور يسهل تخمينها مثل الأسماء الشائعة، عيد ميلادك، رقم جوالك، اسمك الأول أو اسمك الأخير أو الكلمات والأرقام المتسلسلة: ABCD أو QWERTY أو 12345، كما يمكن أن يتم استخدام طرق بديلة مثل استخدام بصمة إصبع اليد أو بصمة العين / الوجه لمزيد من الحماية حال توفر ذلك.



- تغييرها بشكل دوري
- عدم اختيار كلمة مرور مسية على معلومات شخصية
- اختيار كلمة مرور قوية تحوي على مجموعة من الحروف والأرقام والرموز
- عدم مشاركتها
- استخدام كلمة مرور مستقلة لكل حساب

- عدم تدوين كلمات المرور على الأوراق الصغيرة أو خلف البطاقات أو تحت لوحة المفاتيح أو على ركن الشاشة أو ضمن سجل أرقام التواصل بالهاتف.
- احذر من متصفح الأكتاف فهم يتربصون أي فرصة لمشاهدة كتابتك على لوحة المفاتيح وسرقة كلمات المرور.
- أن يتم تأمين البريد الإلكتروني والتطبيقات ببريد إلكتروني وأرقام هواتف استرجاع خاصة وأمنة كما يجب حماية التطبيقات المختلفة بمعايير التحقق الثنائي للوصول (الدخول بخطوتين) والتأكد من إعدادات التشفير للبيانات حال توفرها.
- أن يتم إعداد الخصوصية ضمن برامج التواصل الاجتماعية وعدم إظهار المعلومات الشخصية للعموم وكذلك إظهار المشاركات لكل دون تحديد الأصدقاء أو مجموعات الأصدقاء.
- أن تتم مراجعة الملف الشخصي ومراقبة قائمة الأصدقاء والمضافين ضمن فترات معينة وإتاحة ذلك للأباء والأمهات لمراجعة القوائم بأنفسهم والتأكد من عدم وجود أشخاص غرباء مجهولين الهوية.
- الكثير من الأجهزة الذكية تقوم بحفظ موقع الجهاز خصوصاً عند تواجد خدمات تحديد المواقع GPS فيجب أن يتم الإعداد والحد من هذه الخدمات وعدم السماح بمشاركة مواقعك مع الآخرين حتى لا يتمكن أي غريب أو مجهول معرفة أماكن تواجدك عند استخدام التطبيقات المختلفة ومنع التربص.
- عدم استخدام شبكات الواي فاي اللاسلكية العامة والمفتوحة فهي بيئة شبكية غير آمنة وقد يتم اختراق جهازك وسرقة بياناتك ومعلوماتك وحساباتك وانتهاك خصوصيتك مجرد قبول الانضمام بها.
- عدم مشاركة شبكات الواي فاي اللاسلكية الخاصة بك أو العائلية بالمنزل فبمجرد دخول الغرباء إليها قد يستطيعون اختراق كافة الأجهزة المتواجدة بالشبكة وسرقة المعلومات وفقدان الحسابات وانتهاك الخصوصية.
- عند استخدام الشبكات الافتراضية VPN يجب التأكد من إعدادات الأمان مع مختصي تقنية المعلومات لاستكمال إعدادات الحماية والتشفير والجدار الناري وتوثيق أمن الوصول لشبكات العمل الرسمية.

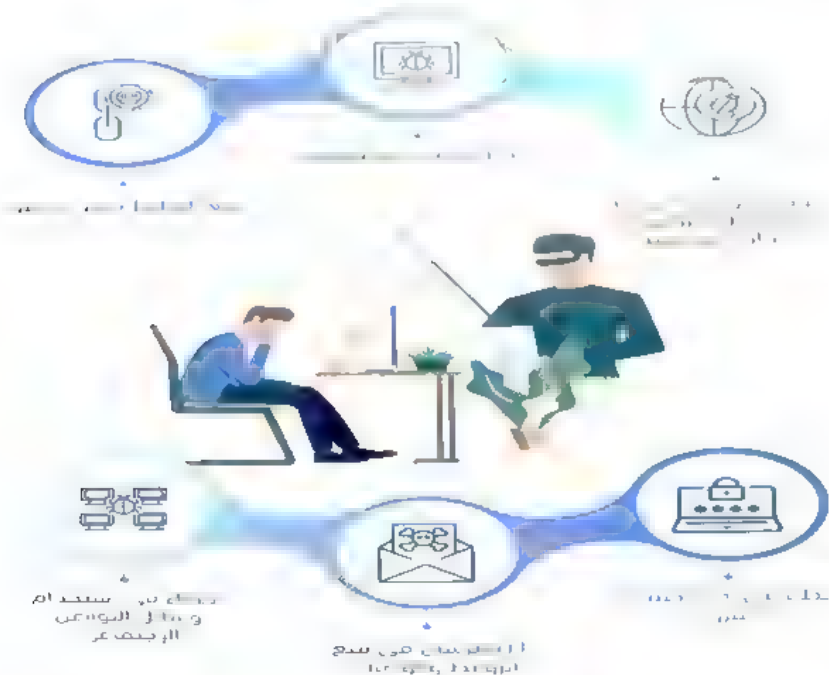


إدراك حالات الخداع والتحايل السيبراني

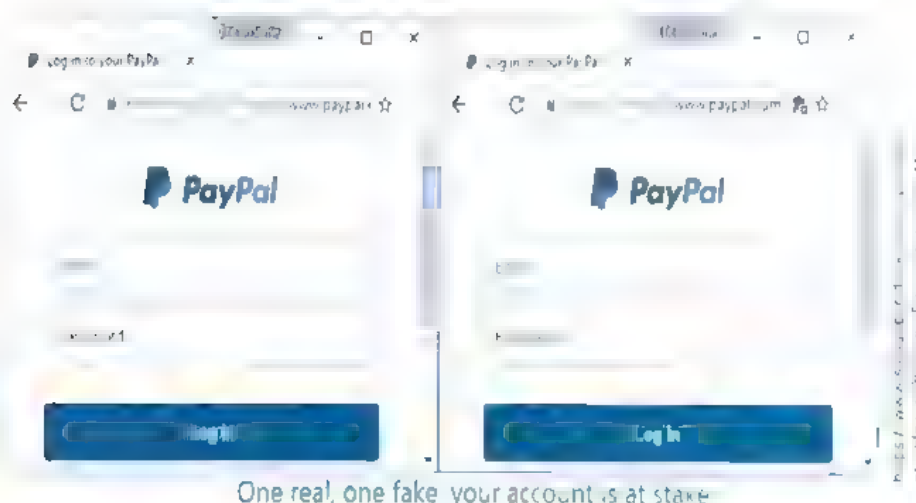
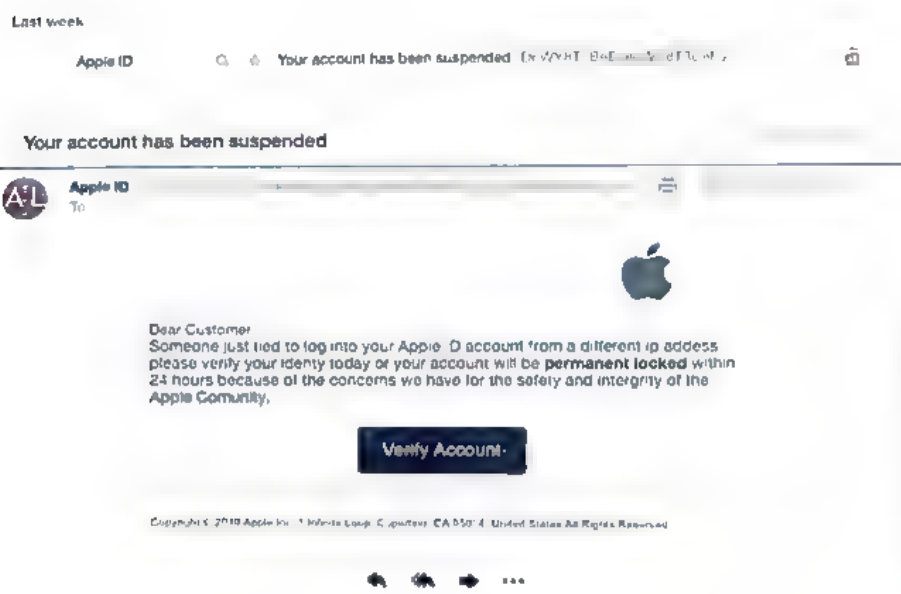
لعل من أحد العوامل المؤثرة على أمن المعلومات في الساحة السيبرانية هو التعامل بحسن النية مع المخترقين والمخادعين حتى تقع الضحية في فخ الاحتيال ومشاركة المعتدين البيانات والمعلومات الحساسة وبذلك تتم سرقة الحسابات وانتهاك الخصوصية وقد تصل إلى سرقة الأموال.

من هنا يجب أن نحرص على ما يلي:

- عند تواجدك في الفضاء السيبراني فتوقع دائماً أن هناك من يراقبك ويحاول خداعك وسرقتك.
- لربما يستغل المعتدين تواجد معلوماتنا الشخصية المتاحة للجميع ضمن برامج التواصل الاجتماعي فيقومون بجمعها وقد يستغلون بعض الأصدقاء لجمع بيانات أكثر منهم عنا وبعدها تبدأ لعبة الاحتيال والحديث معنا وكأنهم أصدقاء وإبداء المساعدة لنا وهم في الحقيقة مخادعين غرضهم الخداع وسرقة البيانات والمعلومات الحساسة منا.
- قد يستغل المعتدي خداعك من خلال جهاز أو حساب صديقك المخترق ويبدأ الحديث معك وكأنه صديقك فعلاً وتبدأ المطالبة بمشاركة المعلومات الحساسة أو طلب المساعدة المالية أو غيرها. هنا يجب أن يتم التأكد من هويته المتحدث والاتصال المباشر بصديقك أو مقابلته وجهاً لوجه خصوصاً في القضايا الهامة.
- وقد يستغل بعض المعتدين حجة الفوز بالجوائز والمسابقات الوهمية وماهي إلا وسيلة أخرى للتحايل وسلب الضحايا معلوماتهم الهامة والشخصية الخاصة للوقوع في فخ يكلفهم الكثير من الخسائر بدلاً من الفوز والربح.



- التزييف والخداع أحد أخطر وسائل الهجوم واصطياد الضحايا، والصور أدناه توضح بعض تلك الطرق، في الصورة الأولى بريد إلكتروني بصيغة رسمية وهوية شركة موثوق بها ولكن من عنوان بريدي مزيف، والثانية توضح تصميم لصفحة شركة باي بال المعروفة ولكن من عنوان رابط مزيف.



أولاً ماذا نعني بالهندسة الاجتماعية؟

الهندسة الاجتماعية (Social Engineering) تعرف بفن التلاعب وخداع المستخدمين حتى يصرحوا ببياناتهم ومعلوماتهم السرية والخاصة لاستغلالها في أغراض الاختراق وسرقة الحسابات وانتهاك الخصوصية وانتحال الشخصية وسرقة الأموال وغيرها من الجرائم المعلوماتية.

يقوم المعتدي باستخدام الذكاء الاجتماعي والصوت البريء وإظهار حسن النية واستعداده في تقديم المساعدة والعون وإيهام الناس بأن التعامل معه سيفيدهم وذلك بتحقيق مصالح لهم مثل تحديث النظام وتطوير الأدوات التقنية وتسريع الخدمات والإنترنت وإصلاح الأعطال وغيرها من الادعاءات ويقوم المعتدي بطلب بعض البيانات السرية بحجة التأكد من هويتهم وأنها مطلوبة من مقدم الخدمة ويقوم بطلب بيانات دخول المستخدم على النظام أو التطبيق وكلمات المرور وأرقام هاتف الجوال وأرقام الهوية الوطنية أو الجواز أو الحسابات البنكية وأرقام البطاقات الائتمانية وغيرها من البيانات الحساسة والتي لا يجب مشاركتها مع أي أحد حفاظاً على سريتها.



النشاط الثالث:

يظهر أحد سيناريوهات الهندسة الاجتماعية وهي بين أحد الطلبة المستخدمين لنظام أو منصة التعليم الإلكتروني المعتمدة من وزارة التعليم وأحد محترفي التصيد الإلكتروني، وقد تعرض الطالب للخداع باستخدام الهندسة الاجتماعية.

محور النقاش: ما هو التصرف الأمثل عند مواجهة هذا الفخ السيبراني؟

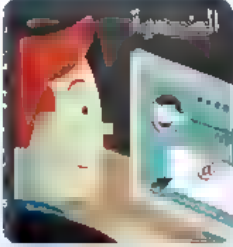
<https://fs7.formsite.com/alibaro/jnuhpeop4n/index.html?1628589658724>



ملاحظة السيناريو يعتبر تخيلي مبني على الخبرات وبعض القصص المشابهة.

النشاط الرابع :

نشاط الهندسة الاجتماعية



عملية الاحتيال تتم عبر إحدى برامج التواصل الاجتماعي
مثل واتس أب أو تليغرام أو غيرها



مرحباً ، أنا اسمي نعيم

أعمل مهندس كمبيوتر في إحدى شركات الدعم الفني المعتمدة من شركة مايكروسوفت ومن قبل وزارة التعليم.

أتواصل معك اليوم بسبب ظهور رسالة من جهازك تطلب تحديث النظام وعمل صيانة دورية لزيادة سرعة الإنترنت ومن بعدها سرعة الدخول على نظام الوزارة وحضور كافة الفصول الافتراضية بسهولة .

أهلاً وسهلاً !! شكراً اخ نعيم

صحيح فأنا أعطي منذ فترة من عدم سرعة الإنترنت وتعلق الجهاز المتكرر في المنصة واحتاج منك أن تخدمني وتحديث جهازي وتنزل كافة الأدوات المجانية لكي أتمكن من استخدام النظام والمنصة بكل يسر وسهولة .

سعد بخدمتكم واحتاج منك بعض البيانات البسيطة لإتمام عملية التحديث والتي تطلبها الوزارة لعمل الإحصاءات وإثبات تقديم الخدمات لكم.

فضلاً إرسال اسم المستخدم وكلمة المرور / إيميلك الشخصي وإيميل ولي الأمر / رقم الجوال ورقم جوال ولي الأمر / يفضل أن تعطيني كذلك أرقام الهوية الوطنية لإثبات حضوركم بالفصول الافتراضية .

اسم المستخدم على المنصة Ahmad
كلمة المرور : AhlMadA20

جوال : 05500000000
جوال ولي الأمر : 05000000000

الهوية : 012012012012
الإيميل : asdggg@gmail.com
إيميل والدي : assdjh@gmail.com

آخر شيء هنالك بعض الخدمات التي وفرتها الوزارة لكم مجاناً وتم دفع قيمتها، ولكن لكي يتم إلزامها لكم بالجهاز نحتاج إلى ما يثبت موافقة ولي الأمر والأمر بسيط هو فقط إدخال رقم البطاقة الانتمائية وتاريخها ورقم التحقق وهي فقط لإثبات الموافقة وإن يتم مسح أي مبلغ منها فالخدمات قد دفعتموها لكم الوزارة بالكامل
شكورة على ذلك

رقم بطاقة العيزا :
2136-9784-6548-6543
اسم صاحب البطاقة : Masud A.
تاريخها : 08/22
رقم التحقق خلف البطاقة : 156

شكراً لكم وأتمنى أن تعطيني خبر أو ما تنتهي وتصلح النظام ..

وآلف شكر لكم .

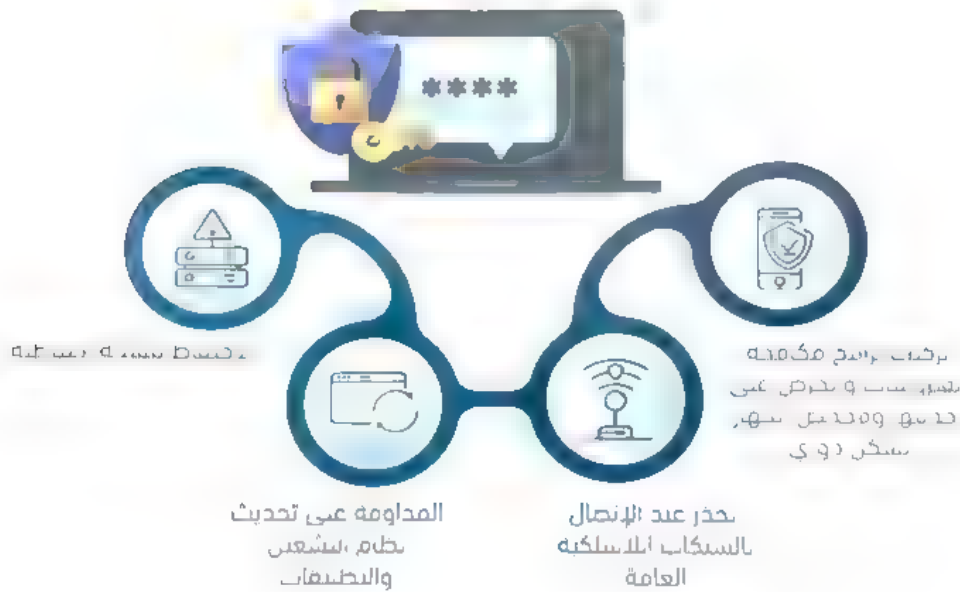
بكل سرور وسنعمل جاهدين لخدمتكم ...

الجلسة الخامسة



ماهي أهم الإرشادات التي يوصي بها المختصين؟

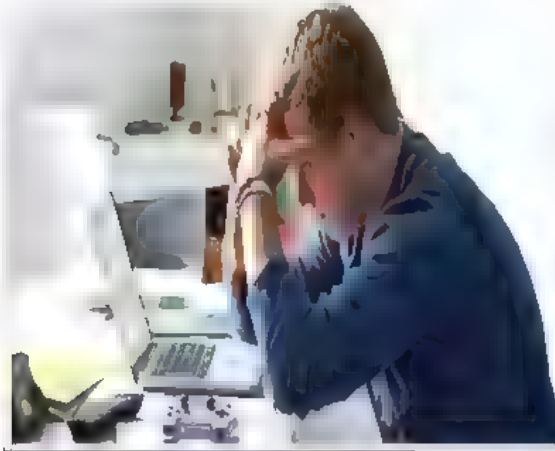
لعله من أهم الأمور هو المحافظة على أمن جهازك وملفاتك و المداومة على ما يلي:



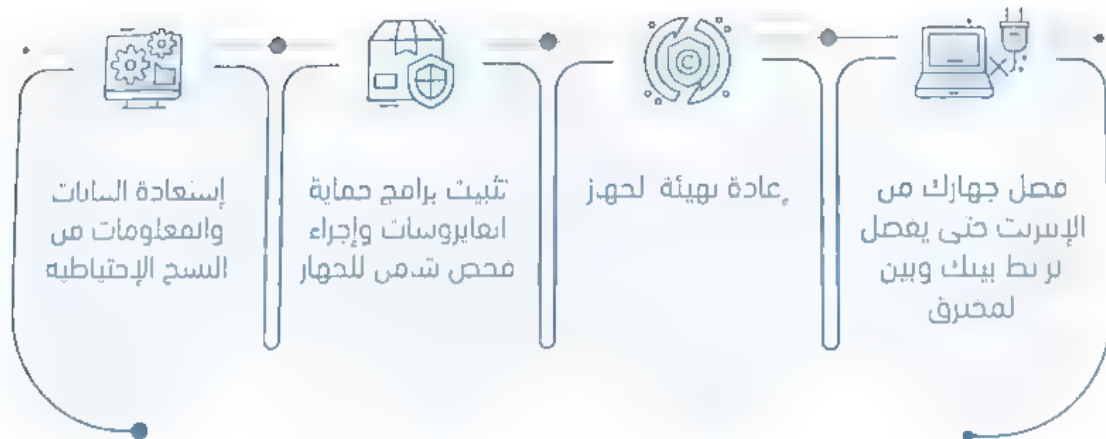
حسناً، ماذا أفعل عندما أتعرض لأي اعتداء إلكتروني؟

- يجب عليك في البداية تجاهل الرسائل من المعتدين والغرباء وحظر الأرقام والحسابات المجهولة.
- يجب التوقف عن مشاركة المعتدي أو المهاجم أو الغرباء بشكل عام أي معلومات خاصة.
- يجب عليك عدم الرد على المعتدي والاعتداء عليه بالمثل فهو سلوك خاطئ قد يضعك في خانة الاتهام ويفقدك حقا في المطالبة بالدفاع.
- كما يجب عدم السكوت عن الاعتداء ويجب أن يتم الإبلاغ عنه وعدم التجاهل في حال استمرار المعتدي بالمضايقة والتهديد لكيلا تكبر المشكلة وتزيد من أثارها السلبية عليك.
- عدم الحرج من نقاش أي حالة اعتداء عليك مع المقربين أو الأصدقاء الثقات، وإن كانت معلومات تخص العمل فيجب إبلاغ المسؤولين في العمل مثل الرئيس المباشر أو من تتقون به كمختص تقنية المعلومات.

- البدء في جمع وحفظ كافة الرسائل المتبادلة كدليل وشاهد يثبت حالة الاختراق أو الاعتداء ونوعه وعدم حذف الأدلة وإن طلب المعتدي ذلك.
- يمكن الدخول على تطبيق "كلنا أمن" واختيار الجرائم المعلوماتية في حال تم تصنيف الاعتداء كجريمة إلكترونية أو معلوماتية.
- يكون رفع بلاغ الجرائم الإلكترونية من خلال التطبيق كلنا أمن ويجب اختيار نوع البلاغ من أحد الخيارات المتاحة بالتطبيق وهي:
 - ذكر نوع التطبيق الذي تم حدوث الاعتداء من خلاله: تويتر، انستغرام، سناب شات، يوتيوب، فيسبوك، أو غيره.
 - كتابة حساب المعتدي مع رابط الحدث ضمن البلاغ وذكر حالة الحساب: هل هو نشط أو غير نشط أو محذوف.
 - شرح وافي عن حالة الاعتداء ورفاق المستندات المساندة والداعمة التي تثبت الحالة.
- الانتظار بعد إرسال البلاغ والتأكد من استلام الرقم المرجعي للبلاغ لبدء الجهات المختصة في التحري واتخاذ ما يلزم نظاماً.
- عدم إبلاغ المعتدي بأنه قد تم رفع بلاغ عنه، كما لا يجب التواصل معه شخصياً عبر أرقام هواتف أو البريد الإلكتروني أو حسابات أخرى.
- يفضل عدم قبول أي إضافات لصداقات مجهولة وذلك لإغلاق فرصة تواصل المعتدي مرة أخرى بعد حظره من خلال حسابات جديدة.
- الإبقاء قريباً مع المختصين ومنحهم فرصة مراقبة الحساب الشخصي لفترة حتى يتم التأكد من سلامة الاستخدام وزوال الخطر.
- العودة إلى استخدام التطبيقات يجب أن يكون بحذر وبشكل آمن بعد معرفة وإدراك كافة المخاطر المحتملة وكيفية منعها والتصدي لها.
- في حال حصول الاعتداء على أحد من أصدقائك أو الأقرباء فلا تتردد بالإبلاغ وإتباع الخطوات السليمة ومساعدتهم، ومساندتهم، ونصحهم، وإرشادهم.



ومن الخطوات التقنية الهامة لاستعادة السيطرة بعد اختراق الجهاز:



وفي حال اختراق أحد الحسابات الخاصة بكم فيجب إتباع النصائح التالية:

● تغيير كلمة المرور الخاص بالحساب الذي تم اختراقه على الفور وبكلمة جديدة



● البحث عن أي تحديثات جديدة للأنظمة والأجهزة والتطبيقات لضمان سد أي ثغرة أمنية قد يمكن استغلالها.

● مراجعة جميع إعدادات الأمان والخصوصية بحساباتكم والتأكد من صحتها.

● الإبلاغ عن الاختراق وتحذير جميع من قد يتمكن المخترق من التواصل معهم منتحلاً شخصية صاحب الحساب المخترق.

● التواصل مع إدارة الحساب أو الشركة أو مسؤول تقنية المعلومات والإبلاغ عن

الاختراق لكي يتمكنوا من فحص الاختراق ومعرفة ما إذا كان هناك ثغرات جديدة قد يمكن استغلالها.

● عدم الاستجابة لأي طلبات جديدة من أي مجهول وتفاذي فتح وتتبع الروابط الغير آمنه والمجهولة المصدر.

كما هنالك الكثير من الجهات المعتبرة والتي تمنح فرصة التواصل المباشر وأخذ المشورة وإرسال الاستفسارات وأخذ الإجابات الموثوقة للمساعدة والدعم والإرشاد، وقد وفرت لنا حكومتنا الرشيدة العديد من المؤسسات التنظيمية والخدمات الإلكترونية لحفظ حقوق المواطنين بشكل عام وذلك لإرشادهم وخدمتهم وحمايتهم. فيجب الحرص على معرفتها والاستفادة منها، من المصادر ما يلي:



- للإبلاغ عن جريمة معلوماتية: يمكن استخدام تطبيق (كلنا أمن)، موقع الأمن العام (moi.gov.sa)

المركز الوطني لإرشادي
سلام السيبراني
SAUDI CERT



- عند وجود أسئلة عن أمن المعلومات: قم بزيارة موقع المركز الوطني للإرشادي للأمن السيبراني (cert.gov.sa)



هيئة الاتصالات وتقنية المعلومات
Communications & Information
Technology Commission

- للإبلاغ عن مشاكل في خدمات الاتصالات: قم بزيارة موقع هيئة الاتصالات وتقنية المعلومات (www.citc.gov.sa)

انترنت السعودية
internet sa



- للإبلاغ عن محتوى معلوماتي سلبي أو سيء: قم بزيارة موقع إنترنت السعودية (internet.sa)



مركز الأخلاق والتقنية
National Center for Digital Ethics and Regulation
NCDER

- للإبلاغ عن محتوى مخل للأداب: قم بزيارة موقع اللجنة الوطنية لتقنين المحتوى الأخلاقي لتقنية المعلومات (ncder.gov.sa)

و عند الحاجة الى الاستشارات النفسية الفورية يمكنكم التواصل مع الجهات التالية:



المركز الوطني
لتعزيز الصحة النفسية

بالتواصل مع مركز اتصال الاستشارات النفسية على الرقم (920033360) من
الأحد إلى الخميس من 8 صباحاً - 4 عصرًا



التواصل مع خط مساعدة الطفل على
الرقم (116111) للاستشارات
الفورية أو التبليغ عن الاساءات التي
تحدث للأطفال



طلب الاستشارة نصياً أو عبر تسجيل
صوتي في أي وقت من خلال تطبيق
قريبون (التطبيق متاح في متجر أبل
وقوقل بلاي)

ملاحظة:

جميع الاستشارات تقدم من قبل مختصين في الجانب النفسي والاجتماعي وبسرية تامة.



نشاط مقياس الممارسات الإلكترونية الخاطئة

يهدف هذا النشاط إلى توعية المتدربين بالمفاهيم الأساسية بالأمن السيبراني ويمكنهم من قياس مدى التقبل أو الرفض لكثير من الممارسات التي تصنف بأنها استخدامات خاطئة:



يعتبر نشاط فردي حيث يقوم المتدرب بالإجابة على كل عبارة إما بالموافقة أو عدم الموافقة ولكافة العبارات.



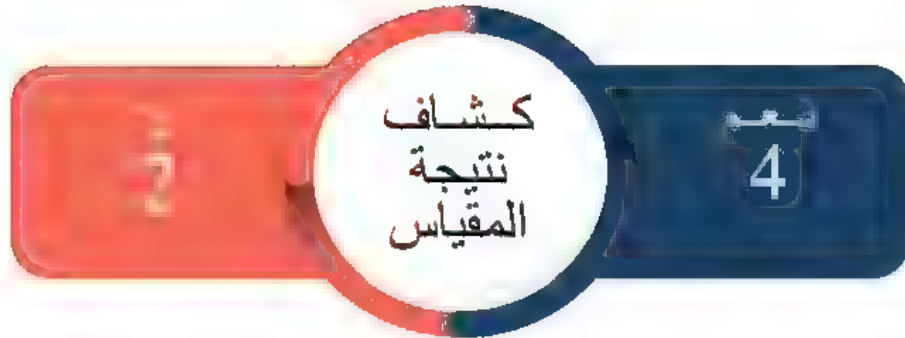
بعد ذلك يقوم المدرب بنقاش نتائج المقياس مع المتدربين ومعرفة فيما إذا كان هنالك تقبل أو رفض أو حياد للممارسات الخاطئة.

المقياس متوفر عبر الإنترنت وإمكانية القياس إلكترونياً من خلال الرابط أدناه:

<https://fs7.formsite.com/alibaro/8emcyeozi2/index.html>



كشف نتيجة حساب المقياس



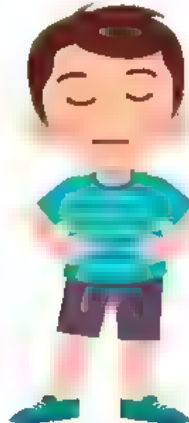
معادلة حساب النتيجة

$$(عدد عبارات نعم \times 4) + (عدد عبارات لا \times 2)$$

ضع/ ضعي نتيجتك هنا



64-52
تعني القبول



50-46
تعني الحياد



44-32
تعني الرفض

من أهمية التطور التكنولوجي في حياتنا أصبح واجب علينا أن نحافظ على معلوماتنا في البيئة السيبرانية لضمان بقائها واستمرارها، ومن هنا نقدم أهم عشر نصائح مسئلة من كتاب الوصايا العشر في الأمن السيبراني (المبيض، ٢٠٢٠):

* الوصايا العشر في الأمن السيبراني *



أولاً: مستوى أمان كلمة المرور يجب التأكد على أن تكون كلمات المرور الخاصة بكم صعبة وغير منطقية ويفضل أن تحمل حروف وأرقام ورمز خاص بكم إن أمكن، كلما كانت كلمة المرور صعبة وغير متوقعة كلما كان من الصعب تفكيك الشفرة الخاصة.



ثانياً: كلمة مرور مختلفة لكل حساب فلا يجب استخدام كلمة مرور واحدة لجميع حساباتكم الإلكترونية، من لديه كلمة مرور واحدة لكل حساباته فهو كمن ينطبق عليه المثل (من يضع البيض في سلة واحدة) فعلى الأقل يجب أن تكون لديك ثلاث أو أربع كلمات مرور قوية.



ثالثاً: التحقق بخطوتين لضمان سلامة حساباتكم من الاختراق ولضمان أيضاً استعادتها بعد فقدان أو تسيان الأرقام السرية يجب عليكم تفعيل خطوات التحقق الثنائي أو التحقق من خطوتين، التحقق الثنائي هو التحقق عن هوية المستخدم من مصدرين مختلفين لضمان إثبات هوية صاحب الحساب الفعلي.



رابعاً: برامج الحماية المعلوماتية يجب ألا تنهائوا في اقتناء برامج الحماية الموثوقة وتحديثها بشكل دوري، ويتوجب عليكم بتحديث برامج الحماية الموجودة على جميع أجهزكم حتى تكون بياناتكم وملفاتكم وشبكاتكم بأمان من جميع البرامج والملفات الضارة.



خامساً: البرامج ذات المصادر غير المعروفة يجب أن لا تقوموا بفتح أو تحميل البرامج ذات المصادر المجهولة أو غير الموثوقة، وذلك لضمان سلامتها وخلوها من أي ملفات ضارة تسمح للمخترقين من خلالها الوصول إلى بياناتكم وأجهزكم الخاصة.



سادساً: تقليد البرامج والرسائل الإلكترونية احذروا التقليد ! هذه العبارة تكتب دائماً على الكثير من المنتجات الاستهلاكية العينية، وذلك لتحذير المستهلكين من وجود بضائع مطابقة للمنتج. أما في عالم التكنولوجيا فيعتبر التقليد هو من أكثر الاختراقات شيوعاً ومن أكثرها حصداً للضحايا.



سابعاً: شبكات WI-FI للأسف هي شبكات انترنت عامة تشكل خطراً شديداً على سلامة أجهزكم وبياناتكم والاشتراك مع الأشخاص المجهولين بشبكة واحدة يشكل ثغرة أمنية سهلة للمخترقين ومما يتيح لهم سرقة العديد من البيانات المسجلة على أجهزكم ويجب علينا عدم مشاركة أجهزتنا بشبكات عامة.



ثامناً: النسخ الاحتياطي من الجيد عمل نسخ احتياطي لبياناتكم بشكل دوري، وذلك لسهولة حفظها والعودة لها في حل تم فقدانها من أجهزكم بسبب حقل تقني أو أمني.. ويفضل أن يكون النسخ الاحتياطي لبياناتكم أن يكون مجاني غير مدفوع وذلك لضمان استمرارية النسخة الاحتياطية للبيانات.



تاسعاً: تحديث البرامج والأنظمة والتطبيقات يجب أن يكون بشكل دوري وفي حل صدور تحديثات لأي منها للحماية المثلى، كما أن تحديث أنظمة أجهزكم وتطبيقاتكم يتيح للشركات والمطورين من تطوير وسائل الحماية وسد الثغرات الأمنية المكتشفة.



عاشرأ: بياناتكم الشخصية المخترقون بالعادة يجمعون معلومات ضحاياهم لتحليلها وتحديد طريقة الاختراق المناسبة ونقاط الضعف والثغرات المتاحة في المواقع التواصل الاجتماعي، لذلك عليكم التقليل من نشر معلوماتكم عبر الإنترنت، فهو يعتبر أمر صحي لأمن معلوماتكم وخصوصيتكم.



وفي الحتام، فيجب أن يكون كل فرد واعي بأهمية الحماية والملكية والخصوصية في الفضاء السيبراني وحماية المعلومات الشخصية والمعلومات المتعلقة بأسرته وأصدقائه وعمله ومنظمته ووطنه وعدم المشاركة الا لمن يستحق بعد التحقق من المعلومات التي يمكن المشاركة بها فكما ليس كل ماء صالح للشرب فليست كل معلومة صالحة للمشاركة. ولنعلم جيداً أن بعد الضغط على إزرار إرسال أصبحت المعلومة ملك المستلم وحتى بعد حذفها من جهازك ويظهر لك البرنامج مسحها فهي في مكان ما بداخل حوادم الشركة المقدمة للخدمة ولها الحق في مشاهدتها وتحليلها ومشاركتها وبيعها في بعض الاحوال، فأحرص أن معلوماتك الشخصية وصورك الجميلة ليست



للعرض والتداول وأن كان البعض يقول الجملة الشهيرة "هل أنا من بين كل الملايين سيتم اخذ صوري" ولما لا يكون استخدام الذكاء الاصطناعي له دور في ذلك بعدد المشاهدات او عدد الاعجاب او المشاركات بالمنطقة وغيرها من المحددات ويتم الاختيار بناء على ذلك. نسبة حدوث ذلك قد تكون ضئيلة، ولكن لا يمكن ان نقول مستحيلة، فالفضاء السيبراني في اتساع دائم وإن لم نحرص فقد نندم وهناك تطور مستمر في وسائل وأساليب الهندسة الاجتماعية والتي زانت من حالات السرقات والتحايل وانتحال الشخصيات والابتزاز وغيرها من الجرائم المعلوماتية، وتقع مسؤولية نشر الوعي والامن على الجميع وتبدأ من المنزل بين الأبناء والاباء والامهات والعائلة بين الأشقاء والأقرباء الى

الموظف والمسؤول في الأعمال والمعلم والمعلمة في المدارس والجامعات وحتى بين الأصدقاء وحتى بين افراد المجتمع من قد نتواصل معهم في الفضاء السيبراني المتسع.

كسر شفرة (Enigma) في الحرب العالمية كان بسبب التهاون لإجراءات الاستخدام الصحيح

فلا تتهاونوا عند الاستخدام والمشاركة حفظكم الله ...

استبانة تقييم البرنامج التدريبي

Workshop evaluation - استبانة تقييم ورشة العمل

Full Name - الاسم الكامل

eMail - البريد الإلكتروني

* اختر افضل اختيار لما يلي - Choose the best answer for each of the following

	Strongly Agree - اتفق بشدة	Agree - اتفق	Neutral - محايد	Disagree - لا اتفق	Strongly Disagree - ينفو بشدة
The presenter(s) communicated clearly كان التواصل مع المدرب واضحاً	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I learned something new - قد تعلمت شيئاً جديداً	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
This course was relevant to my position المعلومات كانت مناسبة لي	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
This course was a valuable use of my time كان البرنامج مفيداً واستغل وقتي جيداً	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The level of received knowledge was enough كمية المعلومات المستلمة كانت كافية	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

How difficult was this course for the amount of material it covered? - لاي مدى كان محتوى المادة العلمية صعباً *

- ☐ Too Difficult - صعب جداً
☐ Difficult - صعب
☐ Average - متوسط
☐ Easy - سهل
☐ Too Easy - سهل جداً

How long was this course for the amount of material it covered? - لاي مدى كان طول المدة المطلوبة لإنهاء البرنامج *

- ☐ Too long - طويلة جداً
☐ Long - طويلة
☐ Average - متوسطة
☐ Short - قصيرة
☐ Too short - قصيرة جداً

Overall, how satisfied were you with this training course? - بشكل عام، ما هو مدى رضاكم عن البرنامج *

- ☐ Very Satisfied - راضٍ جداً
☐ Satisfied - راضٍ
☐ Neutral - محايد
☐ Dissatisfied - غير راضٍ
☐ Very Dissatisfied - غير راضٍ جداً

How likely would you be to recommend this course to a coworker or colleague? - لاي مدى تصحح الموظفين أخذ هذا البرنامج التدريبي *

- ☐ Very Likely - محتمل جداً
☐ Likely - محتمل
☐ Neutral - محايد
☐ Unlikely - مستبعد
☐ Very Unlikely - مستبعد جداً

Comments or Suggestions - هل لديكم أي ملاحظات تحسينية للمستقبل

تتوفر الاستبانة عبر الرابط التالي: <https://fs7.formsite.com/alibaro.kc4eiwlfyy/index.html>

استبانة التقييم البعدي لقياس وعي المتدربين بمفاهيم الأمن السيبراني.
أرجوا قراءة العبارات التالية والإجابة بـ (نعم) حال الموافقة على ما تم ذكره بالعبارة
والاجابة بـ (لا) حال عدم الموافقة عليها:

لا	نعم	العبارة
		أقوم باستخدام برمجيات وتطبيقات خاصة لحماية جهازي من الاختراق والتجسس والفيروسات
		أحتفظ بالبيانات الخاصة بي في أكثر من مكان لتفادي فقدانها أو تلفها
		أقوم بنسخ البيانات الخاصة بي احتياطياً في ذاكرة خارجية وحفظها بـمكان آمن
		أسمح بمشاركة معلوماتي الشخصية للأصدقاء عبر الإنترنت وبرامج التواصل الاجتماعي وغيرها من الوسائل بالفضاء السيبراني
		أسمح بمشاركة معلوماتي الشخصية للغرباء عبر الإنترنت وبرامج التواصل الاجتماعي وغيرها من الوسائل بالفضاء السيبراني
		أسمح بمشاركة بعض معلوماتي الشخصية غير الحساسة للأصدقاء عبر الإنترنت وبرامج التواصل الاجتماعي وغيرها من الوسائل بالفضاء السيبراني
		أسمح بمشاركة بعض معلوماتي الشخصية غير الحساسة للغرباء عبر الإنترنت وبرامج التواصل الاجتماعي وغيرها من الوسائل بالفضاء السيبراني
		أحرص على تجنب مشاركة المعلومات المخالفة للعقيدة، أو الدين، أو القوانين، أو الاعراف، أو التقاليد
		دالما ما اراعي آراء الآخرين ومشاعرهم عند مناقشة موضوع ما عبر الإنترنت
		أصبح لدي وعي كافي بأنظمة المملكة العربية السعودية المتعلقة بالأمن السيبراني يمكنني من التعامل مع الإنترنت وبرامج التواصل الاجتماعي بشكل آمن وصحيح
		أشدد على ضرورة توعية المستخدمين/ الموظفين/ الطلبة بمفاهيم الأمن السيبراني والتعليمات والقوانين والمخالفات والعقوبات المتعلقة باستخدام الإنترنت وبرامج التواصل الاجتماعي
		أؤيد وضع إجراءات وسياسات واضحة لحفظ الأمن السيبراني الخاصة بمشاركة المعلومات ونقلها عبر الإنترنت



قائمة المراجع العربية:

1. الحربي، شيخة عمران ابراهيم. (2019). العوامل الاجتماعية المرتبطة بالجرائم السيبرانية: دراسة ميدانية. رسالة (ماجستير)-جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاجتماعية، قسم علم الاجتماع، تخصص تأهيل ورعاية اجتماعية. رابط:
<https://repository.nauss.edu.sa/handle/123456789/66248>
2. بن عباس، ناصر بن محمد ناصر. (2020). تدابير وقائية مقترحة للوقاية من الجرائم السيبرانية: دراسة ميدانية. أطروحة (دكتوراه)-جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاجتماعية، قسم علم الاجتماع، تخصص علم اجتماع الجريمة. رابط:
<https://repository.nauss.edu.sa/handle/123456789/66908>
3. نظام مكافحة جرائم المعلوماتية. (2007). هيئة الاتصالات وتقنية المعلومات. ص. (1-5). الرابط:
https://www.citc.gov.sa/ar/RulesandSystems/CITCSys/Document/LA_004_20A_20Anti-Cyber%20Crime%20Law.pdf
4. المنتشري، فاطمة يوسف، حريري، رندة. (2020). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للتربية النوعية. مج. 4، ع. 14، يوليو 2020. ص ص. (95-140). الرابط:
<http://search.shamaa.org/FullRecord?ID=260482>
5. المبيض، محمد شاكر. (٢٠٢٠). الوصايا العشر في الأمن السيبراني. الرياض، المملكة العربية السعودية، مطبعة الحميضي.
6. التتمرة آفة لانراها. (٢٠٢١). دليل الأباء الإرشادي للأطفال في العالم الرقمي. وزارة الاتصالات وتقنية المعلومات، المملكة العربية السعودية. ص. ١-٣٤. يمكن الوصول عبر الرابط:
<https://cyberbullying.atta.sa/Parents-guide-for-children-in-the-digital-world-new.pdf>

قائمة المراجع الأجنبية:

1. Aiken, M. (2017). The cyber effect: A pioneering cyber-psychologist explains how human behavior changes online. London, United Kingdom, John Murray Press.
2. Albar, A. A., (2017). Aggression in Cyber Sphere: A Qualitative Study to Explore Saudi Arabian Social Media. Knowledge Discovery and Data Design Innovation, pp. 145-170. Retrieved from https://www.worldscientific.com/doi/abs/10.1142/9789813234482_0008
3. Albar, A. A., (2018). Development of Scales to Measure the Level of Aggression in Saudi Cyber Sphere. A conference paper presented in "The 21st Saudi Computer Society National Computer Conference (SCS-NCC'2018)". Riyadh, Kingdom of Saudi Arabia. pp. 1-8.
doi:10.1109/NCG.2018.8593167. Retrieved from <https://ieeexplore.ieee.org/abstract/document/8593167/references#references>
4. Al-Zahrani, A. M. (2015). Cyberbullying among Saudi's higher-education students: Implications for educators and policymakers. *World Journal of Education*, 5(3), 15-26. Retrieved from <https://files.eric.ed.gov/fulltext/EJ1158405.pdf>
5. Starcevic, V., & Aboujaoude, E. (2015). Cyberchondria, cyberbullying, cybersuicide, cybersex: "new" psychopathologies for the 21st century? *World Psychiatry*, 14(1), 97-100.

الملحق (أ)

[illegible]

أسئلة لازالت لدي (Q)؟

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100
 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200
 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300
 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400
 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500
 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600
 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700
 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800
 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900
 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000

الملحق (ب)

بيانات التواصل المباشر مع باحث/ مؤلف/ معد/ مقدم الحقبة التدريبية:



Royal Commission for Jubail & Yanbu

الهيئة الملكية للجبيل وينبع

د. علي بن عيّدوس بن علي البار
وكيل وكالة التعليم الإلكتروني
وكالة التعليم الإلكتروني
قطاع التعليم – الهيئة الملكية ببنع

مدينة بنع الصناعية – العزيزية - كلية بنع الجامعية – مبنى E – مكتب E2-006

Dr. Ali A. Albar
Managing Director, eLearning Directorate
eLearning Directorate,
Division of Education - Royal Commission Yanbu

Yanbu Industrial City- Yanbu University College- Building (E) – Office (E2-006)

+966-50-552-2558 014-394-61000 (Ext. 1580)

albara@rcyci.edu.sa www.ali-albar.net

WWW.RCJY.GOV.SA

Note: According to the new security policies, I will not be able to receive emails from public email providers (i.e., @gmail, @yahoo, @hotmail, etc.)

